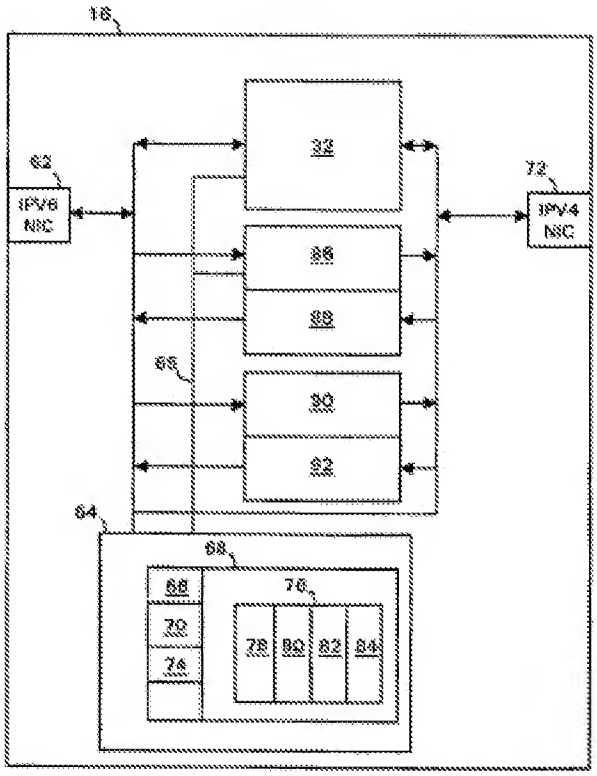
Packet network interfacing

Publication number: CN1376351
Publication date: 2002-10-23
Inventor: HOVELL PETER (GB); KING JOHN ROBERT (GB); PATTERSON JOHN (GB)
Applicant: BRITISH TELECOMM (GB)
Classification:
- international: ***H04L12/46; H04L29/06; H04L29/12;*** **H04L12/46; H04L29/06; H04L29/12;** (IPC1-7): H04L12/56; H04L12/46
- European: H04L29/12A2A1; H04L12/46E; H04L29/06; H04L29/06J
Application number: CN20008013292 20000925
Priority number(s): EP19990307551 19990924

Also published as:
WO0122683 (A3)
WO0122683 (A2)
US7188191 (B1)
MXPA02002828 (A)
CA2382534 (A1)
more >>

Abstract not available for CN1376351
Abstract of corresponding document: **WO0122683**

A method of interfacing, and an interface for use, between two IPv6 domains separated by an IPv4 domain. The interface comprises a protocol converter, an encapsulator/un-encapsulator and a controller. When an IPv6 source wishes to send to a named destination in the other IPv6 domain, the source sends a normal IPv6 address request to its local DNS server, which relays it to an IPv6 name server in the other IPv6 domain. The response message, containing the true IPv6 address of the destination is received at the remote interface, which appends to the resulting protocol converted DNS response message a first additional record containing the true IPv6 address, and a second additional record containing the IPv4 address of that interface. Upon receipt at the other interface, the additional records are stripped off, their contents stored in an entry of a table, and the true IPv6 address written into the address record of the resulting IPv6 DNS response message. When the interface receives a packet from an IPv6 host, it checks whether the destination address matches an entry of its table, and if so sends the packet to the encapsulator together with the IPv4 address of the remote interface. The remote interface extracts the source address and the address of the encapsulating interface and stores these in an entry in its corresponding table for use in encapsulating return packets to the source. If, however, the destination address is recognised as being of IPv4-compatible or IPv4-mapped format, the packet is sent to a protocol converter.



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 12/56
H04L 12/46

[12]发明专利申请公开说明书

[21]申请号 00813292.5

[43]公开日 2002年10月23日

[11]公开号 CN 1376351A

[22]申请日 2000.9.25 [21]申请号 00813292.5
[30]优先权
[32]1999.9.24 [33]EP [31]99307551.4
[86]国际申请 PCT/GB00/03684 2000.9.25
[87]国际公布 WO01/22683 英 2001.3.29
[85]进入国家阶段日期 2002.3.22
[71]申请人 英国电讯有限公司
地址 英国伦敦
[72]发明人 皮特·霍维尔 约翰·罗伯特·金
约翰·帕特森

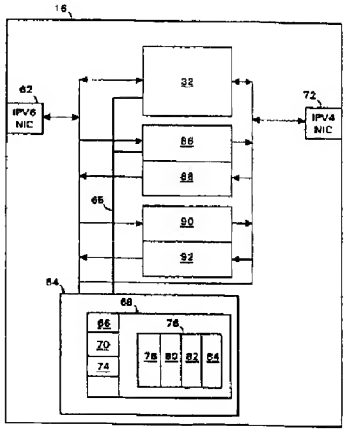
[74]专利代理机构 北京三友知识产权代理有限公司
代理人 李 辉

权利要求书 4 页 说明书 16 页 附图页数 6 页

[54]发明名称 分组网络连接

[57]摘要

一种用于由一个IPv4域分隔的两个IPv6域之间的连接方法和所使用的接口。该接口包括一个协议转换器,一个封装器/解封装器和一个控制器。当一个IPv6源希望向另一个IPv6域中的指定目的地发送时,该源把一个普通IPv6地址请求发送到它的本地DNS服务器,该本地DNS服务器把该请求转发到该另一个IPv6域中的一个IPv6名称服务器。在远程接口接收包含有目的地的真实IPv6地址的响应消息,远程接口把一个包含真实IPv6地址的第一附加记录和一个包含该接口的IPv4地址的第二附加记录附加到所得的协议转换的DNS响应消息上。当在另一个接口接收时,剥除这些附加记录,把它们的内容存储在一个表的一个条目中,并且把真实IPv6地址写入所得的IPv6 DNS响应消息的地址记录。当该接口从一个IPv6主机接收到一个分组时,它校验目的地地址是否匹配于它的表中的一个条目,并且如果是,则把该分组与该远程接口的IPv4地址一起发送到封装器。该远程接口提取源地址和封装接口的地址并把它们存储在它的相应表中的一个条目中,以用于封装返回源的分组。但是,如果识别出目的地地址是与IPv4兼容的或IPv4映射的格式,那么把该分组发送到一个协议转换器。



ISSN1008-4274

权 利 要 求 书

1. 一种用于一个第一网络和一个第二网络之间的接口，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址--此处称为第一类型地址，该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址--此处称为第二类型地址，该接口同时具有第一类型地址和第二类型地址，并且包括:

协议转换器，被设置为把具有根据第一传输协议的格式的消息--此处称为第一类型消息--转换为具有根据第二传输协议的格式的消息--此处称为第二类型消息，反之亦然;

封装装置，被设置为响应与一个第一类型消息一起接收的一个第二类型地址，使用所接收的第二类型地址作为所得的封装第二类型消息的目的地地址，并使用该接口的第二类型地址作为所得的封装第二类型消息的源地址，把所接收的第一类型消息封装为所得的封装第二类型消息的有效负载;

解封装装置，用于解封装一个第二类型消息，以取出它的有效负载；和

接口控制器，被设置为响应接口从第一网络接收的一个第一类型消息，检查从第一网络接收的该第一类型消息的目的地地址，如果它的目的地地址是第一预定格式，则把从第一网络接收的第一类型消息发送到协议转换器，否则，直接或间接地从从第一网络接收的该第一类型消息的目的地地址导出一个第二类型地址，以由封装装置用作一个所得的封装第二类型消息的目的地地址，和把所导出的第二类型地址与从第一网络接收的该第一类型消息一起发送到封装装置。

2. 根据权利要求 1 所述的接口，其中控制器被设置为通过从目的地地址的一个预定子地址字段取出第二类型地址来直接导出第二类型地址。

3. 根据权利要求 1 所述的接口，其中控制器被设置为通过根据目的地地址访问一个具有相关联的第一类型地址和第二类型地址的形式的条目的查找表，并取出一个具有匹配于该目的地地址的第一类型地址的条目的第二类型地

址，来间接导出第二类型地址。

4. 根据权利要求 3 所述的接口，其中查找表的每个条目包括的一个字段中包含一个标识符，该标识符用于标识控制器要把从第一网络接收的第一类型消息发送到协议转换器还是封装装置。

5. 根据权利要求 1 到 4 中任何一个所述的接口，其中封装装置包括多个不同的封装器，每个封装器被设置为根据各自的封装类型操作，并且控制器被设置为依据第一类型消息的目的地地址的格式，把从第一网络接收的第一类型消息发送到所述多个不同的封装器中适当的一个。

6. 根据权利要求 5 所述的接口，在从属于权利要求 3 或权利要求 4 时，其中查找表的每个条目包括的一个字段中包含一个标识符，该标识符用于标识封装的类型。

7. 一种操作一个第一网络和一个第二网络之间的接口的方法，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址--此处称为第一类型地址，该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址--此处称为第二类型地址，该方法包括以下步骤：

检查从第一网络接收的一个第一类型消息的目的地地址；和

如果所接收的第一类型消息的目的地地址是一个第一预定格式，则对所接收的第一类型消息进行协议转换；

否则，使用从所接收的第一类型消息的目的地地址直接或间接导出的一个第二类型地址作为一个所得的封装第二类型消息的目的地地址，根据第二传输协议封装所接收的第一类型消息。

8. 一种操作一个第一网络和一个第二网络之间的接口的方法，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址--此处称为第一类型地址，该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址--此处称为第二类型地址，该方法包括以下步骤：

检查从第一网络接收的一个第一类型消息的目的地地址；和

如果所接收的第一类型消息的目的地地址是一个第一预定格式，则对所接收的第一类型消息进行协议转换；

如果所接收的第一类型消息的目的地地址是一个第二预定格式，则使用从所接收的第一类型消息的目的地地址直接或间接导出的一个第二类型地址作为一个所得的封装第二类型消息的目的地地址，根据第二传输协议封装所接收的第一类型消息。

9. 根据权利要求 8 所述的方法，其中第二预定地址格式包括一个用于标识封装类型的标识符。

10. 根据权利要求 7 到 9 中任何一个所述的方法，其中第一预定格式包括一个第一预定部分，该第一预定部分的内容用于标识所接收的第一类型消息适合于进行协议转换。

11. 根据权利要求 10 所述的方法，其中第一预定格式还包括一个第二预定部分，该第二预定部分的内容等同于用作一个所得的封装第二类型消息的目的地地址的第二类型地址。

12. 根据权利要求 7 到 11 中任何一个所述的方法，其中通过从目的地地址的一个预定子地址字段中取出第二类型地址来直接导出第二类型地址。

13. 根据权利要求 7 到 12 中任何一个所述的方法，其中检查步骤包括以下子步骤：从所接收的第一类型消息取出目的地地址，并根据所取出的目的地地址访问一个查找表。

14. 根据权利要求 13 所述的方法，当查找表包括相关联的第一类型地址和第二类型地址的形式的条目时使用，并且其中取出一个具有匹配于目的地地址的第一类型地址的条目的第二类型地址等同于从所接收的第一类型消息的目的地地址间接导出第二类型地址。

15. 根据权利要求 14 所述的方法，当查找表条目包括一个第一标识符字段--该字段包含一个用于标识第一类型消息是要被进行协议转换还是被封装的标识符--时使用，并且包括以下步骤：从具有匹配于目的地地址的第一类型地

址的条目的第一标识符字段取出该标识符，并检查所取出的标识符与要对所接收的第一类型消息进行协议转换或封装中的哪一个相符。

16. 根据权利要求 14 或 15 所述的方法，当查找表条目包括一个包含用于标识封装类型的标识符的第二标识符字段、并且当有多个封装类型可用时使用，并且包括以下步骤：从具有匹配于目的地地址的第一类型地址的条目的第二标识符字段取出该标识符，并检查所取出的标识符与要对所接收的第一类型消息执行的封装的类型是否相符。

17. 一种用于一个第一网络和一个第二网络之间的接口，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址，该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址，该接口与参照附图描述的相同。

18. 一种操作一个第一网络和一个第二网络之间的接口的方法，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址，该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址，该方法与参照附图描述的相同。

说　　明　　书

分组网络连接

发明领域

本发明涉及一种在一个第一网络和一个第二网络之间的接口，该第一网络根据第一传输协议操作并且具有根据第一编址规则(convention)的网络地址（此处称为第一类型地址），该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址（此处称为第二类型地址）；本发明还涉及从一个这种接口穿过第二网络到另一个这种接口的分组隧穿（tunnelling of packets）；本发明特别（但不是排他地）涉及在由一个因特网协议版本 4（IPv4）域分离的各因特网协议版本 6（IPv6）域中的主机之间的通信。

此处，术语“分组”和“消息”可互换使用，并且具有相同意思，使用“因特网域”作为网络的一个特定例子。

背景技术

在因特网技术中，已经明显看出需要增强最初的传输协议（IPv4），这主要是为了增大可用的地址空间和增加一个分层地址结构。其结果就是 IPv6，IPv6 具有比 IPv4 简化的首部格式，但是与 IPv4 中使用的 32 位地址相比，其使用 128 位地址。

希望对这个一般过渡区域有一个总览的读者可以在 http://www.ietf.org/1id-abstracts.txt 访问作为因特网工程任务组（IETF）的工作文件的一系列因特网草案，一个特别相关的文件是“在 IPv4 世界中引入 IPv6 的指南”<draft-ietf-ngtrans-introduction-to-ipv6-transition-01.txt>，也称为“IPv6 过渡的指南”。

如上所述，本发明涉及隧穿。已知的隧穿技术有两种类型：配置型和自动型。

通过 IPv6 域和 IPv4 域之间的隧穿接口的手动配置以使得从 IPv6 域接收的所有分组被封装在寻址到一个特定隧道终点（tunnel end point）的 IPv4 分组中来产生配置型隧道，即，IPv4 域和包含目的地 IPv6 主机的远程 IPv6 域之间的隧穿接口。

反之，自动型隧道不需要手动配置：隧道终点是自动确定的。在 IETF 内正在研究几种自动型隧穿机制，它们在本领域中称为 6over4，6to4，动态隧穿（Dynamic Tunnelling），和隧道代理（Tunnel Broker）。

如欲得到有关 6over4 的更详细信息，读者可以从 IETF 获得 B. Carpenter 和 C. Jung 在 1999 年 3 月发表的称为 RFC2829 的文件－“无需显式隧道进行的通过 IPv4 域的 IPv6 传输”或它的任何其它形式。

如欲得到有关 6to4 的更详细信息，读者可以从 IETF 获得 B. Carpenter 和 K. Moore 发表的称为 draft-ietf-ngtrans-6to4-02.txt 的文件－“无需显式隧道进行的通过 IPv4 云的 IPv6 域的连接”或它的任何其它形式。

如欲得到有关动态隧穿的更详细信息，读者可以从 IETF 获得称为 draft-ietf-ngtrans-dti-00.txt 的文件。

如欲得到有关隧道代理的更详细信息，读者可以从 IETF 获得称为 draft-ietf-ngtrans-broker-00.txt 的文件。

这些已知的自动型隧穿机制使用多种技术来使隧道能够被自动建立：

ξ 6over4　　多点传送

ξ 6to4　　特殊 IPv6 地址，其中顶层合计符（TLA）包含一个用于 6to4 隧穿机制的标识符，下一层合计符（NLA）包含隧道终点的 IPv4 地址

ξ 动态隧穿　　通过 DNS

ξ 隧道代理　　基于 WWW 的工具

根据本发明的第一方面，提供一种用于一个第一网络和一个第二网络之间的接口，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址（此处称为第一类型地址），该第二网络根据第二传输协议操作并且具有

根据第二编址规则的网络地址（此处称为第二类型地址），该接口同时具有第一类型地址和第二类型地址，并且包括：

协议转换器，被设置为把具有根据第一传输协议的格式的消息（此处称为第一类型消息）转换为具有根据第二传输协议的格式的消息（此处称为第二类型消息），反之亦然；

封装装置，被设置为响应与一个第一类型消息一起接收的一个第二类型地址，使用所接收的第二类型地址作为所得的封装第二类型消息的目的地地址，并使用该接口的第二类型地址作为所得的封装第二类型消息的源地址，把所接收的第一类型消息封装为所得的封装第二类型消息的有效负载；

解封装装置，用于解封装一个第二类型消息，以取出它的有效负载；和

接口控制器，被设置为响应接口从第一网络接收的一个第一类型消息，检查从第一网络接收的该第一类型消息的目的地地址，如果它的目的地地址是第一预定格式，则把从第一网络接收的第一类型消息发送到协议转换器，否则，直接或间接地从从第一网络接收的该第一类型消息的目的地地址导出一个第二类型地址，以由封装装置用作一个所得的封装第二类型消息的目的地地址，和

把所导出的第二类型地址与从第一网络接收的该第一类型消息一起发送到封装装置。

优选地，控制器被设置为通过从目的地地址的一个预定子地址字段取出第二类型地址来直接导出第二类型地址。

另选地，控制器被设置为通过根据目的地地址访问一个具有相关联的第一类型地址和第二类型地址的形式的条目的查找表，并取出一个具有匹配于目的地地址的第一类型地址的条目的第二类型地址，来间接导出第二类型地址。

优选地，地址转换表的每个条目包括的一个字段中包含一个标识符，该标识符用于标识控制器要把从第一网络接收的第一类型消息发送到协议转换器还是封装装置。

封装装置可以包括多个不同的封装器，每个封装器被设置为根据各自的封

装类型操作，并且控制器被设置为确定从第一网络接收的第一类型消息的目的地地址是否是相应的多个预定格式之一，并且如果是，则把从第一网络接收的第一类型消息发送到对应于这一个预定格式的封装装置。

优选地，地址转换表的每个条目中包括的一个字段中包含一个标识符，该标识符用于标识封装的类型，控制器要把从第一网络接收的第一类型消息发送到协议转换器还是封装装置。

根据本发明的第二方面，提供一种操作一个第一网络和一个第二网络之间的接口的方法，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址（此处称为第一类型地址），该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址（此处称为第二类型地址），该方法包括以下步骤：

检查从第一网络接收的一个第一类型消息的目的地地址；和

如果所接收的第一类型消息的目的地地址是一个第一预定格式，则对所接收的第一类型消息进行协议转换；

否则，使用从所接收的第一类型消息的目的地地址直接或间接导出的一个第二类型地址作为一个所得的封装第二类型消息的目的地地址，根据第二传输协议封装所接收的第一类型消息。

根据本发明的第三方面，提供一种操作一个第一网络和一个第二网络之间的接口的方法，该第一网络根据第一传输协议操作并且具有根据第一编址规则的网络地址（此处称为第一类型地址），该第二网络根据第二传输协议操作并且具有根据第二编址规则的网络地址（此处称为第二类型地址），该方法包括以下步骤：

检查从第一网络接收的一个第一类型消息的目的地地址；和

如果所接收的第一类型消息的目的地地址是一个第一预定格式，则对所接收的第一类型消息进行协议转换；

如果所接收的第一类型消息的目的地地址是一个第二预定格式，则使用从

所接收的第一类型消息的目的地地址直接或间接导出的一个第二类型地址作为一个所得的封装第二类型消息的目的地地址，根据第二传输协议封装所接收的第一类型消息。

优选地，第二预定地址格式包括一个用于标识封装类型的标识符。

第一预定格式可以包括一个第一预定部分，该部分的内容用于标识所接收的第一类型消息适合于协议转换。

第一预定格式还可以包括一个第二预定部分，该部分的内容等同于用作一个所得的封装第二类型消息的目的地地址的第二类型地址。

优选地，通过从目的地地址的一个预定子地址字段取出第二类型地址来直接导出第二类型地址。

优选地，检查步骤包括以下子步骤：从所接收的第一类型消息取出目的地地址，并根据所取出的目的地地址访问一个查找表。

更优选地，在当查找表包括相关联的第一类型地址和第二类型地址的形式的条目时所使用的方法中，取出一个具有匹配于目的地地址的第一类型地址的条目的第二类型地址等同于从所接收的第一类型消息的目的地地址间接导出第二类型地址。

在当查找表条目包括一个第一标识符字段（该字段包含一个用于标识第一类型消息是要被进行协议转换还是被封装的标识符）时使用的方法中，可以包括以下步骤：从具有匹配于目的地地址的第一类型地址的条目的第一标识符字段取出该标识符，并检查所取出的标识符与要对所接收的第一类型消息进行协议转换或封装中的哪一个相符。

在当查找表条目包括一个包含用于标识封装类型的标识符的第二标识符字段、并且当有多个封装类型可用时使用的方法中，可以包括以下步骤：从具有匹配于目的地地址的第一类型地址的条目的第二标识符字段取出该标识符，并检查所取出的标识符与要对所接收的第一类型消息执行的封装的类型是否相符。

已经知道，协议转换器用于使 IPv6 主机能够把消息发送到 IPv4 主机。当在一个 IPv6 域中激活一个新 IPv6 主机时，该 IPv6 主机采用称为邻居发现（Neighbourhood Discovery）（ND）的技术来找出它可以直接通信的主机的身份。它广播一个包含它的 IPv6 网络地址的 ND 消息，并且每个接收到该消息的主机发送一个包含该主机的 IPv6 网络地址的应答消息。由于该域使用一种底层传输机制，比如使用介质访问控制（MAC）地址的以太网，每个接收该 ND 消息的主机将取出该新主机的 IPv6 网络地址以及该新主机的 MAC 地址，并且新主机将从每个应答消息中取出该发送主机的 IPv6 网络地址和它的 MAC 地址。

现在，新主机构造一个 ND 表，在该 ND 表中每个条目对应于一个相邻主机并且包括一个第一部分和一个第二部分，第一部分的形式是该相邻主机的 128 位 IPv6 地址，第二部分的形式是相关联的 MAC 地址。

该 IPv6 域与一个邻近的 IPv4 域之间的接口装置（包含协议转换器）也接收到该 ND 消息并发送一个应答消息，并且该新主机将在 ND 表中产生一个特殊的缺省条目，其第一部分由 128 个零（在变型中，它们都是一）形成，其第二部分由该接口装置的 MAC 地址形成。

因此，当该新主机要把一个消息发送到它的域中的一个其他主机时，它构造一个 IPv6 消息并访问它的 ND 表以取出与目的地地址相关联的 MAC 地址。然后以已知方式把该消息封装在一个以太网分组内，并通过底层以太网传输机制把它发送到目的地主机。

另一方面，如果该主机构造一个 IPv6 消息（其目的地地址的形式是一个与 IPv4 兼容或 IPv4 映射的地址），即一个用于相邻 IPv4 域中的一个 IPv4 主机的消息，那么在 ND 表中将找不到该目的地地址。在此情况下，访问算法将返回缺省条目的 MAC 地址，并且将把该消息发送到协议转换器。

协议转换器只能在 IPv6 和 IPv4 消息的首部的对应字段之间转换。例如，当一个 IPv6 消息的首部中的一个字段在一个 IPv4 消息的首部中不具有对应字段时，或反之亦然，那么该字段中的信息将在协议转换过程中丢失。

如上所述，已经知道隧穿技术用于使 IPv6 主机在处于相互间隔的域中时能够在其间进行通信。在此情况下，接口装置包含一个隧穿机制而不是一个协议转换器。应该理解，在此之前，为了使一个 IPv6 主机能够与 IPv4 主机和远程的 IPv6 主机通信，需要该 IPv6 主机和该域接口是双堆栈（dual stack），即同时具有 IPv4 和 IPv6 通信能力。如果一个 IPv6 主机不是双堆栈，它的访问算法将只返回用于缺省条目的单个 MAC 地址。如果网络管理已经决定该 IPv6 主机能够与 IPv4 主机通信，该地址将是一个协议转换器的输入端口的 MAC 地址，而如果网络管理已经决定该 IPv6 主机能够与 IPv6 主机通信，该地址将是一个隧穿机制的输入端口的 MAC 地址。该缺省条目 MAC 地址不会是协议转换器和隧穿机制的公共的输入地址。

附图说明

下面将参考附图对本发明的特定实施例进行说明，其中：

图 1 是连接两个隔离的 IPv6 域的 IPv4 域的示意图；

图 2 是一个边界路由器的示意图；

图 3 是一个 IPv6 DNS 响应消息的示意图；

图 4 是转换图 3 的 IPv6 DNS 响应消息得到的 IPv4 DNS 响应消息的示意图；

图 5 是转换图 4 的 IPv4 DNS 响应消息得到的 IPv6 DNS 响应消息的示意图；

图 6 是显示用于 6to4 隧穿技术的特殊 IPv6 地址的格式的示意图。

具体实施方式

在图 1 中，一个 IPv4 域 10 分隔一个第一 IPv6 域 12 和一个第二 IPv6 域 14，第一 IPv6 域 12 根据本发明等同于一个根据第一传输协议操作、并具有根据第一编址规则的网络地址的第一网络，第二 IPv6 域 14 根据本发明等同于一个根据第一传输协议操作、并具有根据第一编址规则的网络地址的第三网络。IPv4 域 10 中的主机只是 IPv4，IPv6 域 12 和 14 中的主机只是 IPv6。

IPv4 域 10 根据本发明等同于一个根据第二传输协议操作、并具有根据第二编址规则的网络地址的第二网络。为简化图示，未示出 IPv4 主机，并且每个 IPv6 域 12 和 14 中仅示出一个 IPv6 主机（如以下所述，分别是 28 和 30）。

第一 IPv6 域 12 通过边界路由器 16A 连接到 IPv4 域 10，第二 IPv6 域 14 通过边界路由器 16B 连接到 IPv4 域 10。边界路由器 16B 与边界路由器 16A 相同，分别等同于一个接口。

IPv4 域 10 包含一个完整的域名系统（DNS）20，其包括多个 DNS 服务器 22，图中只示出两个 DNS 服务器 22A 和 22B，并且 IPv6 域 12 和 14 包含各自的 DNS 服务器 24 和 26。

假设第一 IPv6 域 12 中的一个主机 28 希望把一个分组发送到第二 IPv6 域 14 中的一个主机 30。因此，在该事务中，主机 28 被称为源主机 28，主机 30 被称为目的地主机 30。

源主机 28 知道目的地主机 30 的名称，因此它以已知方式构造一个用于请求目的地主机 30 的 IPv6 地址的 IPv6 DNS 请求消息（未示出）。源主机 28 把该 DNS 请求消息作为一个循环请求发送到它的本地 DNS 服务器，本实施例中的该本地 DNS 服务器是 DNS 服务器 24。DNS 服务器 24 将以已知方式把多个重复的 DNS 请求消息（未示出）发送到 DNS 20，直到它获知 DNS 服务器 26。最终，一个 DNS 请求消息（未示出）将到达 DNS 服务器 26 以请求目的地主机 30 的 IPv6 地址。

当该 DNS 请求从第一 IPv6 域 12 通过边界路由器 16A 传送到 IPv4 域 10 时，它由一个协议转换器（PC）32A 处理（见图 2），并经历 IPv6/IPv4 转换。相应地，当 DNS 请求从 IPv4 域 10 通过边界路由器 16B 传送到第二 IPv6 域 14 时，它由一个协议转换器 32B 处理，并经历 IPv4/IPv6 转换。

协议转换器 32A 和 32B 遵从被称为网络地址转换-协议转换（NAT-PT）的规范。它们在 IPv4 和 IPv6 地址之间转换，并且在该话路期间保持状态，IPv4 和 IPv6 请求消息与 DNS 响应消息之间的转换（包括 IP 首部和 DNS 有效负载

信息的转换）由一个应用层网关（ALG）控制。在本领域中，DNS 响应消息的一个另选术语是 DNS 答复消息。

如欲了解更多信息，读者可以从因特网工程任务组（IETF）获得 G. Tsirtsis 和 P. Srishuresh 发表的一个名称为“网络地址转换-协议转换（NATPT）”的文件 draft-ietf-ngtrans-natpt05.txt 及其任何变型版本。

DNS 服务器 26 以一个 IPv6 DNS 响应消息 34 来响应请求目的地主机 30 的 IPv6 地址的 DNS 请求消息（见图 3），该响应消息 34 具有常规格式的目的地地址字段 36、源地址字段 38 和包含有目的地主机 30 的 IPv6 地址的响应地址记录 40。

该 IPv6 DNS 响应消息 34 通过第二 IPv6 域 14 到达边界路由器 16B，在此把它转换为一个 IPv4 DNS 响应消息 42（见图 4），该响应消息 42 包括目的地地址字段 44、源地址字段 46、响应地址记录 48，并且根据本发明，还包括附加记录 50 和 52，该消息 42 通过 IPv4 域 10 到达边界路由器 16A，在此把它转换为一个 IPv6 DNS 响应消息 54 然后发送到源主机 28，该响应消息包括 54 包括目的地地址字段 56、源地址字段 58 和响应地址记录 60。DNS 响应消息（以其各种形式，即 34，42 和 54）在域 10，12 和 14 中所经过的路线取决于每个域中的 DNS 配置，但是它必须按上述顺序经过边界路由器 16B 和边界路由器 16A。

为简便起见，术语“字段”和“记录”在本说明书中同义地和可互换地使用，尽管在本领域中通常认为字段是一个记录的一个组成部分。

当边界路由器 16B 通过它的 IPv6 网络接口控制器 62B 接收到 IPv6 DNS 响应消息 34 时，把该响应消息 34 并行馈送到协议转换器 32B 和控制器 64B，并且还馈送到封装器 86B 和 6to4 封装器 90B。控制器 64B 通过控制线 65A 连接到协议转换器 32B、封装器 86B 和 6to4 封装器 90B 的控制输入，并且通过在控制线 65A 上设置一个合适的地址来选择这些装置中适当的一个。

控制器 64B（i）识别所接收的消息是一个 DNS 响应消息并使能协议转换

器 32B，（ii）从响应记录 40 中取出 IPv6 地址并把该消息写入一个由它的内部存储器 68B 的一部分形成的存储单元 66B 中；（iii）把边界路由器 16B 的 IPv4 地址（即，在边界路由器 16B 的隧道终接终点的 IPv4 地址）写入一个也是由它的内部存储器 68B 的一部分形成的存储单元 70B 中；（iv）从协议转换器 32B 接收所转换的 DNS 响应消息 42；附加作为第一附加记录的存储单元 70B 的内容和作为第二附加记录的存储单元 68B 的内容；和（v）把所得的 IPv4 DNS 响应消息 42 发送到一个 IPv4 网络接口控制器 72B，以通过 IPv4 域 10 传输到边界路由器 16A。

在一个变型中，仅把所接收的 IPv6 DNS 响应消息 34 馈送到控制器 64B，控制器 64B 把该消息写入一个由它的内部存储器 68B 的一部分形成的存储单元 74B 中。然后控制器 64B（i）从响应记录 40 取出 IPv6 地址并把该消息写入存储单元 66B；（ii）把边界路由器 16B 的 IPv4 地址写入存储单元 70B；（iii）通过取出存储单元 66B 的内容并附加作为第一附加记录 50 的存储单元 70B 的内容和作为第二附加记录 52 的存储单元 66B 的内容，来产生一个修改的 IPv6 DNS 响应消息；和（iv）把这个修改的 IPv6 DNS 响应消息发送到协议转换器 32B。协议转换器 32 的 ALG 只处理该 DNS 响应消息的首部和地址响应记录以产生所得的 IPv4 DNS 响应消息 42，即，它允许附加记录保持不变。

应该理解，把所接收的消息直接馈送到协议转换器 32B 并由控制器 64B 在控制线 65A 上把一个使能信号发送到协议转换器 32B 在逻辑上等同于在上述变型中由控制器 64B 把所接收的消息发送到协议转换器 32B，并且等同于根据本发明把消息发送到协议转换器 32B。

当边界路由器 16A 通过它的 IPv4 网络接口控制器 72A 接收到 IPv4 DNS 响应消息时，把它并行馈送到协议转换器 32A 和控制器 64A。

控制器 64A（i）从协议转换器 32A 接收输出的 IPv6 DNS 响应消息，该响应消息包括目的地地址字段 56、源地址字段 58、响应地址记录 60 和附加记录 50，52；和（ii）从第二附加记录 52 取出 IPv6 地址（即目的地主机 30 的真实

IPv6 地址），并把它插入该输出消息的响应地址记录 60，而不是把协议转换器 32A 已经产生的用于目的地主机 30 的与 IPv4 兼容的 IPv6 地址插入。然后控制器 64A 剥除附加记录 50，52，并把所得的 IPv6 DNS 响应消息 54（见图 5）发送到边界路由器 16A 的 IPv6 网络接口控制器 62A 以传输到源主机 28。

此外，控制器 64A 被设置为从第一附加记录 50 取出隧道终接终点的 IPv4 地址，以产生目的地主机 30 的 IPv6 地址到 IPv4 隧道终接终点的地址的映射，并把该映射存储在一个由控制器 64A 的内部存储器 68A 的一部分形成的 IPv6/隧道终点表 76A 中（即产生一个条目），该表 76A 等同于本发明的一个查找表。

在一个变型中，在附加记录 50，52 的内容被取出之前把它们从 DNS 响应消息中剥除。在另一个变型中，附加记录保持在 DNS 响应消息中，但是这不如把它们剥除那样有效率。在当前实施例中，IPv6/隧道终点表 76A 中的每个条目包括第一元素 78A，第二元素 80A，第三和第四元素 82A 和 84A，第一元素 78A 包括一个对应目的地主机 30 的 IPv6 地址，第二元素 80A 包括隧道终接终点的 IPv4 地址（即边界路由器 16B 的 IPv4 地址），这些内容将在后面说明。

在接收到所得的 IPv6 DNS 响应消息 54 时，源主机 28 从它的地址记录 60 中取出 IPv6 地址，并存储它以用于把数据分组发送到目的地主机 30。

源主机 28 以已知方式为这些数据分组的每一个产生一个包括源地址字段和目的地地址字段的首部，并把所取出的 IPv6 地址写入目的地地址字段中。

当在边界路由器 16A 接收到这些数据分组的每一个时，控制器 64A 取出目的地地址，并根据所取出的目的地地址，访问 IPv6/隧道终点表 76A。如果有一个与一个条目的第一元素 78A 的内容的匹配，控制器 64A 从该条目的第二元素 80A 中取出对应的 IPv4 隧道终接终点，并命令一个封装器 86A 把该分组封装到一个 IPv4 分组中。因此，封装器 86A 把一个已经插入了它自己的 IPv4 地址的 IPv4 首部附加到源字段中，并把所取出的 IPv4 隧道终接终点地址附加到目的地字段中。在此实施例中，封装器 86A 存储它自己的 IPv4 地址以用于上述目的。在变型中，控制器 64A 存储该 IPv4 地址，并且在命令转发器 86A

进行封装时把它和所取出的 IPv4 隧道终接终点地址一起传送到封装器 86A。

在此实施例中，封装器 86A 被设置为直接从边界路由器 16A 的 IPv6 网络接口控制器 62A 接收分组，但是它在得到控制器 64A 的命令之前不进行封装。在一个变型中，如果存在一个匹配，控制器 64A 直接从 IPv6 网络接口控制器 62A 接收分组并把它传送到封装器 86A。在实践中，当边界路由器 16A 接收到一个分组时，控制器 64A 把它写入它的内部存储器 68A 的一个存储单元中，并且控制器 64A 将把相关存储单元的地址与一个命令封装器 86A 访问该存储单元的指令一起传送到封装器 86A。

当在边界路由器 16B 接收到封装 IPv4 分组时，边界路由器 16B 的解封装器 88B 剥除 IPv4 首部并取出该 IPv4 分组的有效负载（即，解封装来自源主机 28 的原始 IPv6 分组），并把该 IPv6 分组发送到目的地主机 30。控制器 64B 还产生源主机 28 的 IPv6 地址与隧道始发终点（即，始发边界路由器 16A 的 IPv4 地址）之间的一个映射（在它的 IPv6/隧道终点表 76B 中），这二者是分别从 IPv6 首部的源地址字段和 IPv4 首部的源地址字段取出的。

当目的地主机 30 返回一个应答分组时，边界路由器 16B 的控制器 64B 从所接收的应答分组取出目的地地址 “IPv6 主机 28”，根据所取出的目的地地址访问它的 IPv6/隧道终点表 76B（即，搜索一个匹配元素 78B），取出对应的 IPv4 地址（元素 80B），并命令一个封装器 86B，使用刚刚从 IPv6/隧道终点表 76B 的元素 80B 取出的 IPv4 隧道始发终点地址把应答分组封装到一个寻址到边界路由器 16A 的解封装器 88A 的 IPv4 分组中。当在边界路由器 16A 接收到这个 IPv4 分组时，解封装器 88A 进行解封装以取出该应答分组，并且边界路由器 16A 把所取出的应答分组发送到源主机 28。

现在源主机 28 和目的地主机 30 正处于一个话路中，在该话路中 IPv6 分组通过刚刚在边界路由器 16A 和 16B 之间建立的隧道在源主机 28 和目的地主机 30 之间传送。

上述机制用于一个 IPv6 主机（其在一个隔离的 IPv6 域中）通过一个中间

的 IPv4 域与另一个 IPv6 主机（其在另一个隔离的 IPv6 域中）进行通信，而无需知道另一个 IPv6 主机在哪里，并且源 IPv6 主机的操作与它与在它自己的 IPv6 域中的另一个 IPv6 主机进行标准通信程序时没有任何不同。在源 IPv6 主机本地的 DNS 服务器通过 IPv4 域向与目的地 IPv6 主机处于相同的网络上的 IPv6 DNS 服务器进行一个请求，并且边界路由器自动建立把隧道终点和边界路由器之后的 IPv6 主机的 IPv6 地址相关联的各个映射。

在另选实施例中，IPv6/隧道终点表 76A 中的某些条目可以由网络运营商的管理人员创建。这称为隧道的手动配置，并且在管理人员在以后的日子改变隧道之前该隧道是永久不变的。

如图 2 所示，边界路由器 16A 还包括一个 6to4 隧穿封装器 90A（和 6to4 隧穿解封装器 92A），并因此可以与一个被同样使能的边界路由器互通，尽管在变型中这些可以被省略。用于该技术的特殊 IPv6 地址 94（见图 6）具有三部分的格式，其中具有 32 位的第一部分 96 是一个唯一地标识该分组要由 6to4 隧穿技术进行隧穿的前缀，具有 32 位的第二部分 98 是 6to4 隧道终点的 IPv4 地址，具有 64 位的第三部分 100 被称为接口 ID，其是目的地主机的修改后的 MAC 地址。第二部分 98 等同于本发明的目的地地址的预定子地址字段。

在具有一个不同的隧穿封装器的变型中，为相同目的使用一个不同的前缀。

在这些实施例的某些变型中，控制器 64A 被设置为识别所取出的一个接收的分组的目的地地址中的该前缀的存在，以从它的第二部分 98 中取出 6to4 隧道终点的 IPv4 地址，并命令 6to4 隧穿封装器 90A 使用所取出的 IPv4 地址处理所接收的分组。这等同于直接导出第二类型地址。另选地，6to4 隧穿封装器 90A 被设置为取出特殊 IPv6 地址并从它的第二部分 98 中取出 6to4 隧道终点的 IPv4 地址。

如上所述，在控制器 64A 被设置为执行前缀识别的情况下，所要识别的前缀被存储在它的内部存储器 68A 的一个存储单元中，并且该存储单元可以是

IPv6/隧道终点表 76A 的一个条目或一个条目的一部分。

解封装器 88B 和 92B 具有各自的 IPv4 地址，对应的封装器 86A 和 90A 在产生它们各自的封装分组时使用该 IPv4 地址。

在具有多个不同封装器（例如 86，90）的边界路由器的优选布置中，控制器 64A 根据一组匹配准则访问 IPv6/隧道终点表 76A 以覆盖可能的情况范围。这些情况是

（a）已经由上述 DNS 请求技术建立了一个隧道，并且在 IPv6/隧道终点表 76A 中存在一个 IPv6 目的地专用 IPv6/IPv4 条目；

（b）已经由一种已知隧穿技术建立了一个隧道，并且在 IPv6/隧道终点表 76A 中存在一个 IPv6/IPv4 条目，其中第一元素 78A 具有的第一部分的形式是一个对应于该隧穿技术的特定前缀；

（c）网络管理人员已经手动配置了边界路由器 16 以使用到另一个边界路由器（可以是边界路由器 16B 或与再一个 IPv6 域（未示出）相关联的一个不同的边界路由器（未示出））的 6to4（或 6over4）定义一个到一个特定 IPv6 目的地主机的隧道，并且在此情况下 IPv6/隧道终点表 76A 具有的一个条目的第一元素 78A 是该目的地主机的与 IPv4 兼容的（或 IPv4 映射的）地址；

（d）网络管理人员已经手动配置了边界路由器 16A 以使用到另一个边界路由器（可以是边界路由器 16B 或与再一个 IPv6 域相关联的一个不同的边界路由器）的 6to4（或 6over4）定义一个到未指定的 IPv6 目的地主机的隧道，并且在此情况下 IPv6/隧道终点表 76A 具有的一个条目的第一元素 78A 的形式是 6to4（或 6over4）前缀后跟该另一个边界路由器的 IPv4 地址后跟空字符，并且在某些变型中，该条目的第二元素 80A 包含空字符，而在另外有些变型中，该条目的第二元素 80A 包含该另一个边界路由器的 IPv4 地址；和

（e）该表包含的一个条目的第一元素 78A 是一个通用的与 IPv4 兼容的或 IPv4 映射的 IPv6 地址，即，它的前 8 位都是零，并且最后 32（或者在一个变型中，48）位是空字符（零），第二和第四元素 80A 和 84A 包含空字符，并且

第三元素 82A 包含标识符“PC”。

控制器 64A 以如下方式使用它的 IPv6/隧道终点表 76A 来确定一个所接收的分组的适当处理。

如果控制器 64A 发现一个条目的第一元素 78A 匹配于完整取出的目的地地址，那么取出该条目的第二元素 80A 的内容并用作 IPv4 目的地地址，即，边界路由器 16B 的 IPv4 地址，隧道终点。此外，取出该条目的第三元素 82A 的内容并用于校验所取出的 IPv4 目的地地址和由边界路由器 16A 接收的分组是否要由封装器 86A 处理。第三元素 82A 的内容或者是用于封装器 86A，90A 的标识符（例如，“EN”）或者是用于协议转换器 32A 的标识符（例如“PC”）。作为再一个校验，该条目的第四元素 82A 包含一个用于封装类型的标识符。换句话说，对于一个匹配于该完整取出的目的地地址的条目，如上所述，封装类型标识符将是“DNS”以表示要使用该封装器 86A。

如果控制器 64A 发现一个条目的第一元素 78A 的前 32 位匹配于所取出的目的地地址的前 32 位（即特殊 6to4 前缀部分），那么校验该条目的第三和第四元素 82A 和 84A（分别是“EN”和“6to4”），从该条目的第二元素 80A 中取出 IPv4 目的地地址并利用由边界路由器 16A 接收的分组发送以由封装器 90A 处理。这等同于从该目的地地址的预定子地址字段间接取出第二类型地址。

如果所取出的目的地地址是与 IPv4 兼容的或 IPv4 映射的，即该分组要进行协议转换以用于一个 IPv4 目的地，那么它的前 80 位将都是零，并且随后的 16 位将都是零（如果该地址是与 IPv4 兼容的），或者都是一（如果该地址是 IPv4 映射的）。因此控制器 64A 校验它的 IPv6/隧道终点表 76A 是否包含一个其第一元素 78A 的前 80 位都是零的条目。这样一个条目的第二元素 80A 的内容将都是空字符，因为不涉及隧道；并且这样一个条目的第四元素 84A 的内容将都是空字符，因为不涉及封装。取出该条目的第三元素 82A 的内容并用于校验所取出的 IPv4 目的地地址和由边界路由器 16A 接收的分组要由协议转换器 32A 处理。在此情况下，第三元素 82A 的内容是一个用于协议转换器 32A 的标识符

（例如“PC”）。

在其他变型中，控制器 64A 被设置为与原先一样访问 IPv6/隧道终点表 76A，并且只在检测到与一个条目的匹配时才对 6to4 隧穿封装器 90A 发出命令，并且在此情况下，控制器 64A 把特殊 IPv6 地址传送到 6to4 隧穿封装器 90A，或者另选地、控制器 64A 提取 6to4 隧道终点的 IPv4 地址并把它传送到 6to4 隧穿封装器 82A，或者控制器 64A 再一次在检测到这样一个匹配时，取出该匹配条目的元素 80A。该元素 80A 包含 6to4 隧道终点的 IPv4 地址，该 IPv4 地址是由控制器（或手动地）在产生该条目时插入元素 80A 的。

在上述实施例中，源主机 28 的本地 DNS 服务器是 IPv6 DNS 服务器 24，但是在另选实施例中，它可以是 DNS 20 的 IPv4 服务器 22 之一。在这种另选实施例中，尽管主机 28 可以发送一个用于获得主机 30 的 IPv6 地址的 DNS 请求消息，并且根据本发明，建立一个穿过 IPv4 域 10 的隧道，但是这种情形不是对称的，因为主机 30 无法作为一个源并建立一个穿过 IPv4 域 10 到达主机 28 的相应隧道。对于一个根据本发明的方法要成为可连接的(即作为目的地的)IPv6 主机，该 IPv6 主机的本地 DNS 服务器应该是一个与该 IPv6 主机处于相同的 IPv6 域的 IPv6 DNS 服务器，这是因为 DNS 响应消息必须经过与该 IPv6 主机相邻的边界路由器以便能够建立该隧道。换句话说，DNS 请求消息必须经过 IPv4 域，并且不在一个用作所希望的目的地 IPv6 主机的本地 DNS 服务器的 IPv4 DNS 服务器处停止。

说 明 书 附 图

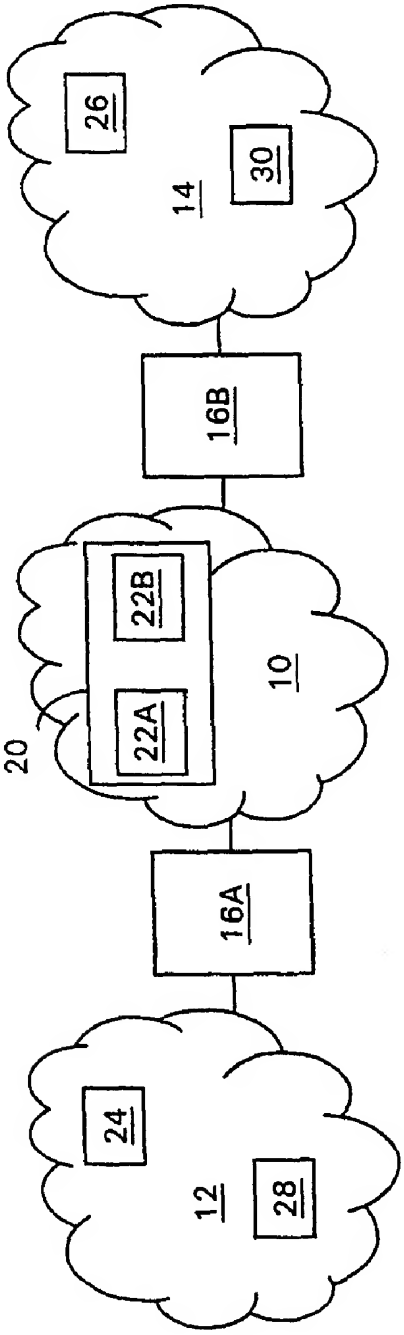


图 1

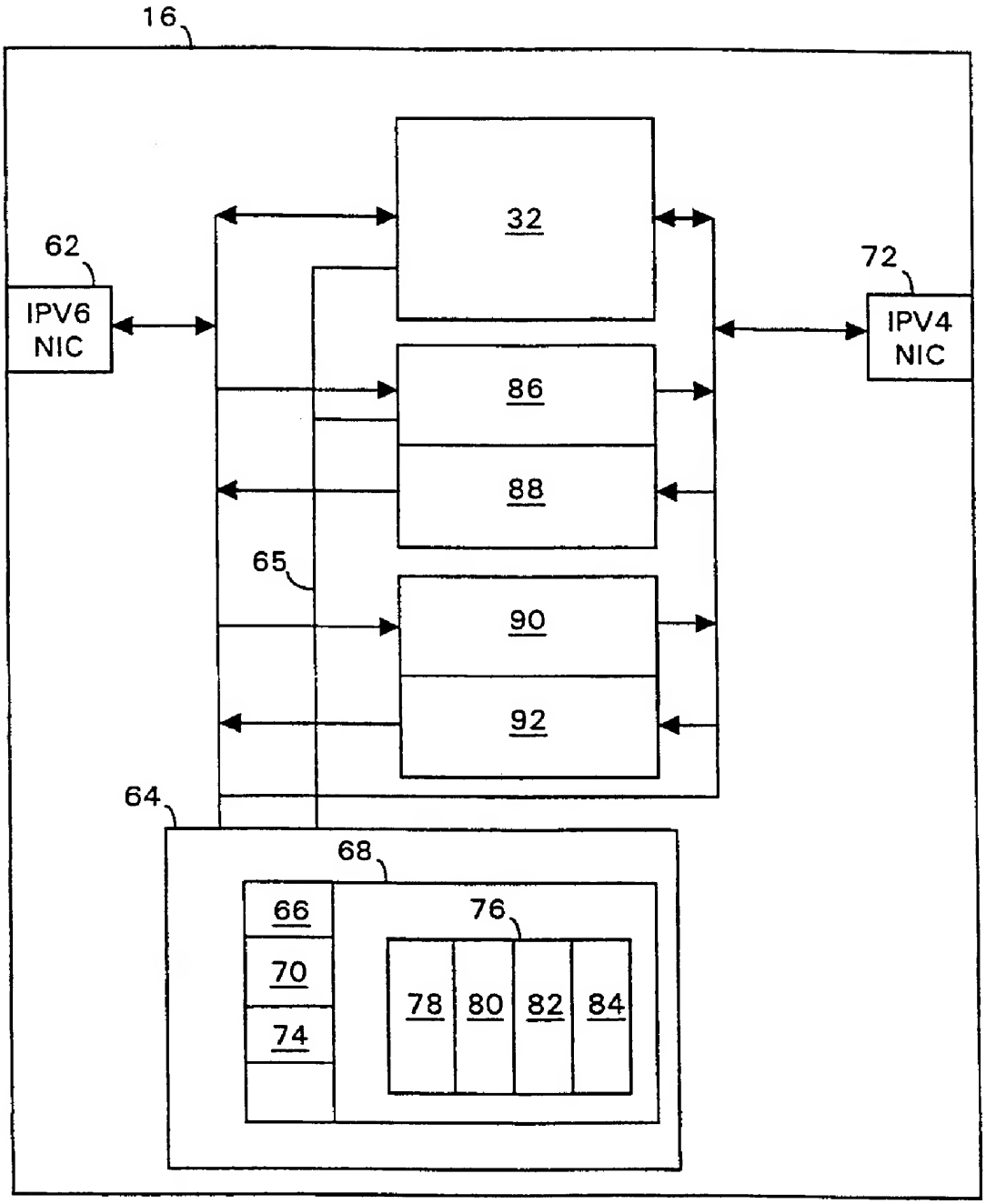

16
32
62
IPV6
NIC
72
IPV4
NIC
86
88
65
90
92
64
68
66
76
70
74
78
80
82
84

图 2

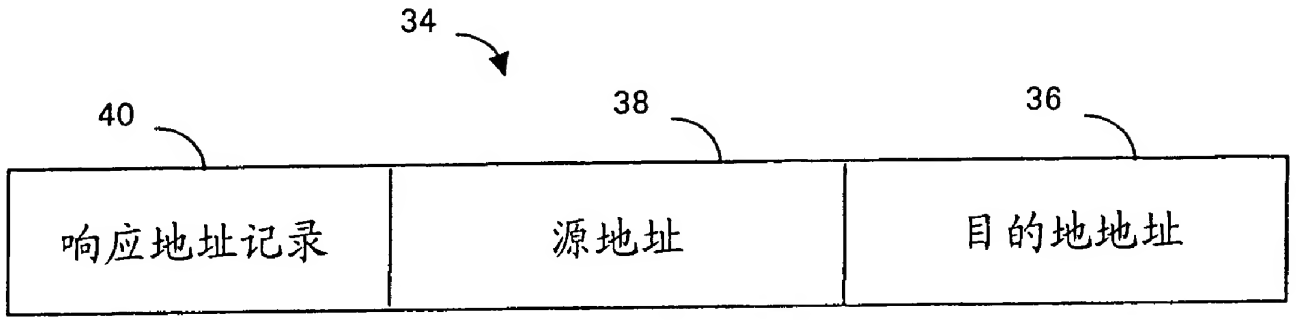


图 3

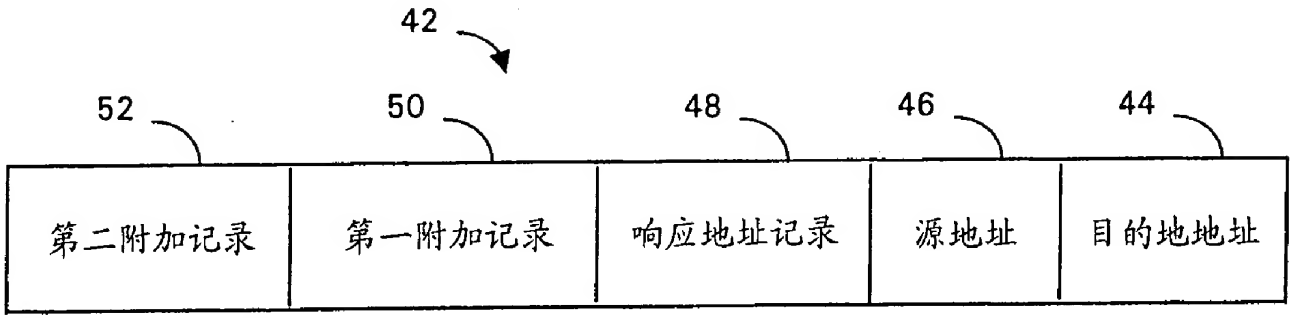


图 4

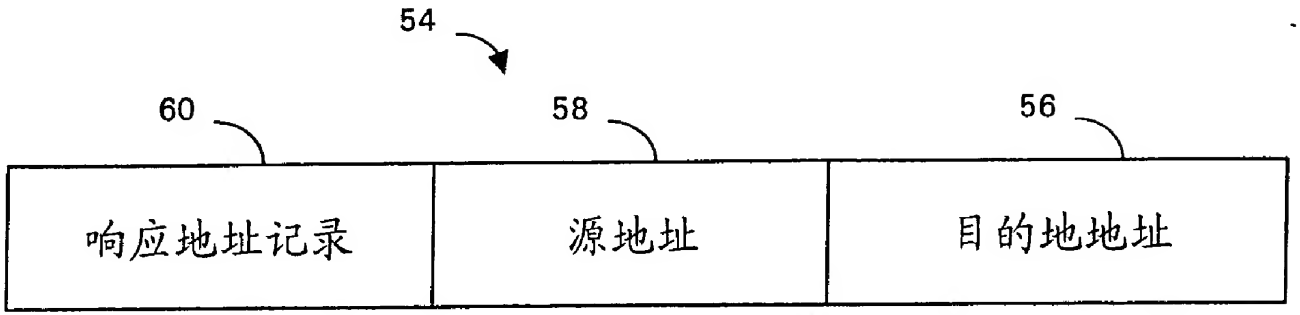


图 5

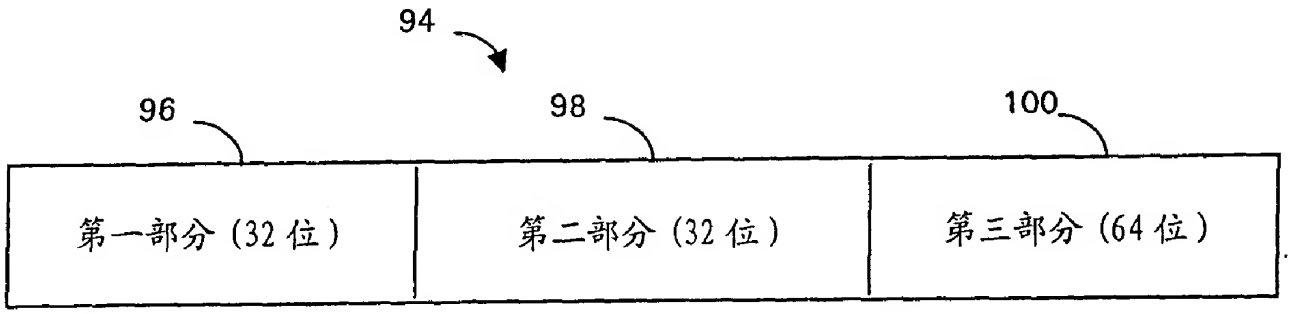


图 6